METHOD TO USE SECURE PASSWORDS IN AN UNSECURE PROGRAM ENVIRONMENT

ABSTRACT OF THE DISCLOSURE

During power up initialization, security data such as passwords and other sensitive data which are stored in a lockable memory device are read and copied to protected system management interrupt (SMI) memory space, subject to verification by code running in the SMI memory space that the call to write the security data originates with a trusted entity. Once copied to SMI memory space, the security data is erased from regular system memory and the lockable storage device is hard locked (requiring a reset to unlock) against direct access prior to starting the operating system. The copy of the security data within the SMI memory space is invisible to the operating system. However, the operating system may initiate a call to code running in the SMI memory space to check a password entered by the user, with the SMI code returning a "match" or "no match" indication. The security data may thus be employed after the lockable memory device is hard locked and the operating system is started.